Impacts of NIST Standards and Specifications

Hildegard Ferraiolo

PIV Project Lead

NIST ITL Computer Security Division

Hildegard.ferraiolo@nist.gov

ICAM Information Sharing Day

March 16, 2014

Impacts of NIST Standards and Specifications

Clustered Topics:

Cluster #1: Mobility, PIV and Authentication

Draft NIST SP 800-157, *Derived PIV Credentials*, Draft NIST IR 7981, *Mobile, PIV, and Authentication*, Draft NIST SP 800-166, *Derived PIV Credential Test Requirements*, NIST SP 800-79, *Guidelines for the Accreditation of PIV Card Issuers and Derived PIV Credential Issuers*

Cluster #2: PIV Card and Infrastructure:

Draft NIST SP 800-73-4, *Data Model &Interfaces for PIV, Draft NIST SP 800-85-2 PIV Card and Interface Test Requirements,*

Impacts of NIST Standards and Specifications

Topic Cluster 1:

Mobility, PIV and Authentication

Draft SP 800-157 – Derived PIV Credential for Mobile Devices

Scope:

- The Derived PIV Credential is an additional PIV Credential to satisfy HSPD-12's 'Common Identification' mandate
- Provide PIV-enabled authentication services on the mobile device to authenticate the mobile device owner to remote systems

Draft SP 800-157:
Addressing a Gap for Remote Authentication with Mobile

PIV Assurance Level Required by Application/Resource	PACS	LACS Local Workstation Environment	LACS Remote/Network System Environment
LITTLE or NO confidence	VIS, CHUID	CHUID*	
SOME confidence	PKI-CAK, SYM-CAK	PKI-CAK	PKI-CAK,
HIGH confidence	BIO	BIO	**PKI-Derived** **(for Mobile Devices)**
VERY HIGH confidence	BIO-A, OCC-AUTH, PKI-AUTH	BIO-A, OCC-AUTH, PKI-AUTH	PKI-AUTH, **PKI-Derived** **(for Mobile Devices)**

Yellow = Environments for the PIV Card Credentials and their authentication mechanisms.

Red = Environments where the new “PKI-Derived” authentication mechanism for Mobile Devices applies.

Draft SP 800-157 – Derived PIV Credential for Mobile Devices

Motivation:

- PIV Cards have been geared towards traditional computing platforms (laptop, desktop)
- For newer computing devices (mobile devices), the use of the PIV Card for e-authentication to remote IT resources is challenging and requires bulky add-on readers

Goal: To provide alternative approaches to PIV-enabled remote e-authentication with mobile device - without PIV Card and add-on readers.

Draft SP 800-157 – Derived PIV Credential for Mobile Devices

Integrated Security Tokens for Mobile Devices:

- Mobile Device Software tokens (current)
- MicroSD tokens (current)
- USB security tokens (near term)
- UICC tokens (near term)
- Embedded Hardware (near term)

Benefits:

- Derived PIV Credential - leverages identity proofing and vetting processes of PIV cardholder
- It's integrated -> better user experience

Considerations:

- Provisioning and management of mobile device specific credential
- Limited mobile OS and application support (MicroSD, USB, UICC)

Draft SP 800-157 – Derived PIV Credential for Mobile Devices

SP 800-157 defines a Derived PIV Credentials for the Security Tokens:

- Define the Derived PIV Credential (a PKI-based credential)
- Both LoA-3 (software) and LoA-4 (hardware) Derived PIV Credential are possible
- Key size and algorithm options are the same as for the PIV Authentication private key
- Defines Derived PIV Credential Lifecycles: Derivation, Issuance, Maintenance (re-key/re-issuance) and Termination

Draft SP 800-157 also includes:

- How to include an optional Digital Signature Key and the Encryption Key in the Derived PIV Credential's security token (Appendix A)

Draft SP 800-157 – Derived PIV Credential for Mobile Devices – Lifecycle Processes

Derivation & Initial issuance:

- Derivation of Derived PIV Credential is based on proof of possession of the PIV card
- Issuance of a LoA-4 credential is in person, while issuance of an LoA-3 allows for remote issuance

Maintenance (rekey and re-issuance):

- Remote rekey to a LoA-3 Derived PIV Credential token
- Remote rekey to a LoA-4 Derived PIV Credential token when rekeying to the same token
- Issuance of a Derived PIV Credential to a new (replacement) token can be done remotely for LoA-3 credential and in-person for an LoA-4 credential
- Derived PIV Credential is unaffected by loss, theft or damage to the Subscriber's PIV Card.

Termination:

- The subscriber is no longer eligible for a PIV Card or is no longer in need of a Derived PIV Credentials
- If token can be collected, then zeroize the private key or destroying the token. Otherwise, revoke the PIV Derived Authentication certificate.

Draft NIST IR 7981
Mobile, PIV, and Authentication

A Companion Document to Draft SP 800-157

- Analyzes different approaches to PIV-enable mobile devices
  - Includes the use of PIV Cards with mobile devices in addition to Derived PIV Credentials
- Points out benefits and considerations (pros/cons) for each approach
  - Example: UICC approach requires cooperation with MNO
- Approximates when these approach might become available
  - Categorized approaches in ‘current’ and ‘near term’ solutions
- Includes Recommendations
  - Hardware rooted solutions provide better security
  - Software solution are available now – NIST IR 7981 recommends complementing these by hardware-backed mechanism to protect the private key of the Derived PIV Credential when not in use (the hybrid solution)
  - In the longer-term, NIST IR recommends adoption of hardware-supported security mechanisms in mobile devices, such as the Roots of Trust (SP 800-164) to support stronger assurance of identity

Mobile, PIV and Authentication

- **Both Draft SP 800-157 and NIST IR 7981 are available for public commenting**
- **Instructions to comment are provided at: http://csrc.nist.gov/groups/SNS/piv/announcements.html**

- **Public comment period closes April 21st**

Draft SP 800-157 Associated Documents

- **Draft SP 800-166 Derived PIV Credential Test Requirements**
  - Specifies derived test requirements for the Derived PIV Credential and its security token (Data Model, and Interfaces)
  - Portability: Removable security tokens ((USB, microSD, UICC) should be portable from one device to another.
  - Align publications close to publication schedule of SP 800-157

- **Test Tool based on SP 800-166 (TBD)**

- **SP 800-79-2 Guidelines for the Accreditation of PIV Card Issuers and Derived PIV Credential Issuers (under development)**
  - **Target Draft Publication Date: May 2014**

Impacts of NIST Standards and Specifications

Topic Cluster 2: PIV Card

A PIV Card Issuer's Perspective:
The FIPS 201-2 Compliant PIV Card

FIPS 201-1

Mandatory

- PIV Authentication
- CHUID
- Biometric (fingerprints)

Optional

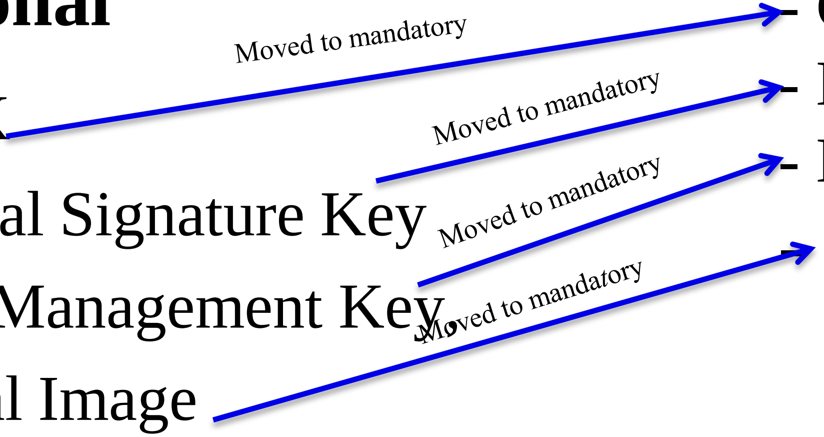
- CAK
- Digital Signature Key
- Key Management Key,
- Facial Image

FIPS 201-2:

Mandatory

- PIV Authentication
- CHUID
- Biometric (fingerprints)
- CAK
- Digital Signature Key,
- Key Management Key

Facial Image



PIV Card Interfaces: Contact, Contactless

FIPS 201-2 Compliant PIV Card+

- **A FIPS 201-2 compliant PIV card with newly introduced optional* features (+)**

Mandatory

- PIV Authentication
- CHUID
- Biometric (fingerprints)
- CAK
- Digital Signature Key,
- Key Management Key
- Facial Image

Optional

New: OCC, Biometric (iris)

PIV Card Interfaces: Contact, Contactless and new optional Virtual Contact Interface (VCI)

*Other optional features from previous specification might also be present (Key History, Printed Information etc.)

Availability of FIPS 201-2 Compliant PIV Cards

- *FIPS 201-2 Compliant PIV Cards:*
  - *Cards implement all mandatory features*
  - *Available today and listed at FICAM TP site*
- *FIPS 201-2 Compliant PIV Cards+ (with new optional Add-On Feature):*
  - *Cards implement all mandatory features plus some (or all) optional features*
  - *+ features (optional features) are the main focus and effort in SP 800-73-4*
  - *Available when:*
    - *Technical specification for optional features are detailed (SP 800-73-4)*
    - *Test requirements are defined (SP 800-85A/B)*
    - *Optional feature are implemented by vendors and have been tested (NPIVP) as per SP 800-85 A/B.*
    - *PIV Card+ will be listed at:*
      - *NIST: http://csrc.nist.gov/groups/SNS/piv/npivp/validation.html and*
      - *FICAM TP: http://www.idmanagement.gov/ficam-testing-program*

Thank you

Questions?

Hildegard Ferraiolo
PIV Project Lead
NIST ITL Computer Security Division
hildegard.ferraiolo@nist.gov